Secure Scan Design Using Redundant Scan Register

Sabyasasachee Banerjee[1], Pranay Kumar Saha[2]
[1] Department of Computer Science & Engineering,
Heritage Institute of Technology, Anandapur, Kolkata, W.B., India,
E-mail: *sabyasasachee.banerjee*@gmail.com
[2] Department of Computer Science & Technology,
B. P. C. Institute of Technology, Krishnagar, Nadia, W.B., India,
E-mail: pranay.kumar.saha@gmail.com

Abstract— **Cryptographic VLSI chip has a significant role to resist the attacks which is the growing customer concern of hardware security. Redundancy introduces a great amount of randomness & non linearity in any kind circuitry (combinational or sequential). We introduce a new type of redundancy in sequential circuits to make redundant scan registers that are indistinguishable with the original scan registers. They are sequentially undetectable as well as redundant, which makes it highly secured. The approach is only to replace the original scan registers to modified redundant scan registers called *RScR*.**

Keywords— **Functional equivalence, Isomorphic redundancy, *RScR***

I. INTRODUCTION

In the modern era, security of crypto-chips is a major concern. Currently, all communication, networking, database management systems and financial application use cryptographic methods. In crypto chips generally the keys are stored in the sequential circuits. In order to improve the testability of sequential circuits scan chains are popularly used. But scan chains open side channel for cryptanalysis. With improved control and access to the chip, vulnerability to attacks also increases. Due to this, scan chains can be used to steal important information such as intellectual property (IP) and secret keys of cryptographic chips [2, 3]. The possibility of scan-based side-channel attacks adds to an already growing customer concern of hardware security. Fundamentally, the problem lies on the inherent contradiction between testability and security for digital circuits. Hence, there's a need for an efficient solution such that both testability and security are satisfied.

II. REVIEW WORK

In order to solve this tricky problem of efficiently testing without compromising the security, some techniques have been proposed.

Lock and Key Technique: In this proposed method [7] scan chain architecture with mirror key register was used to provide both testability and security. Two modes of operations introduced, insecure mode and secured mode. In the insecure mode, crypto chip can be switched between the test mode and the normal mode. However, when a crypto chip is in the secure mode, it can only stay in the normal mode. The switching between insecure mode and secure mode at any time can be done through a power off reset. But this method has the following shortcomings:

a) There are certain devices (example credit cards, cell-phone sim-cards, and access cards) where even after turning the power off the information exists inside the chip. This information can be extracted from those devices having in the insecure mode.

b) Speed testing or on-line testing is not possible.

c) There are critical systems that remain on continuously (like satellite monitoring system). In such cases device's power-off is not possible. Hence testing in such a scenario requires alternative solutions.

Karri's method of secure scan design:

Consisting two copies of the secret key:

- Secure key: hardwired or in secure memory.
- Mirror Key (MKR): used for testing.

&Two modes of operation: Insecure and Secure

Insecure mode: secure key is isolated, MKR [1] is used and debug allowed. Secure mode: secure key is used and debug disabled. To support the secure-scan DFT architecture, here MKRs are used to isolate the secret key from the data path and control path performing the crypto algorithm. Such MKRs work like normal registers during insecure mode, and test vectors can be scanned in and the test result can be scanned out. When the circuit is in the secure mode, the MKRs load the secret-key information and the contents of MKRs cannot be scanned out until being reset. Here a test access port (TAP) controller controls the working mode of the crypto chip.

Partial scan technique using balanced structure: The balanced structure [9] is a structure for testable sequential circuits. We adopt a partial scan to make a *kernel* balanced, where a kernel is the portion of the circuit excluding the scan chains. The partial scan protects non-scan registers completely from scan-based attacks. In addition, we introduce a mechanism to confuse the kernel logic in test mode to protect scan registers. The method makes the circuit behavior in test mode completely different from normal mode.

Vlm-Scan *Technique*: It is a Vlm-Scan [10] that utilizes some flip-flops in a scan chain for authentication to move to test mode. The circuit can proceed to test mode only if the proper sequence of test keys are scanned in to the used flip-flops. It is better because the test controller can be tested; however, a long test key sequence is still needed.

DOI: 01.IJSIP.03.01.81

III. Preleminaries

A. de Bruijn graph:

A de Bruijn graph represents a state transition graph of a shift register. Shown in Fig.1

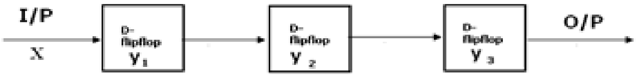
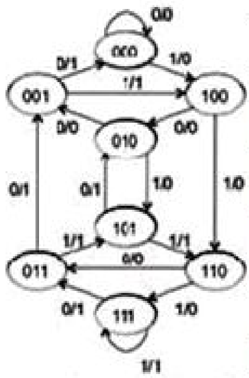


Fig1. abc$_1$ Scan register

The corresponding de Bruijn graph and state table are shown in Fig. 2 and Table 1 respectively

TableI . State Table of fig.1



X	0	1
$Y_1Y_2Y_3$		
S_0 (000)	S_0/0	S_4/0
S_1 (001)	S_0/1	S_4/1
S_2 (010)	S_1/0	S_5/0
S_3 (011)	S_1/1	S_5/1
S_4 (100)	S_2/0	S_6/0
S_5 (101)	S_2/1	S_6/1
S_6 (110)	S_3/0	S_7/0
S_7 (111)	S_3/1	S_7/1

Fig2. de Bruijn graph

B. Functional Equivalence:

A k-stage modified shift register is called *functionally equivalent* [6] to the k-stage shift register if the de Bruijn graph of the modified shift register is isomorphic to that of the shift register and the input and output assignments are the same as those of the shift register. (State assignment is not necessarily the same.) The functional equivalent de Bruijn graph of Fig. 2 is shown in Fig. 3

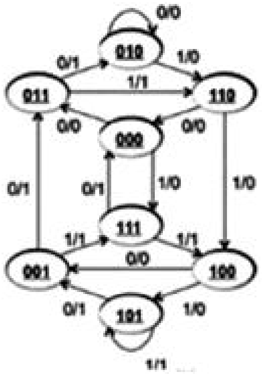


Fig3. Functional equivalent de Bruijn graph

C. Isomorphic redundancy:

An isomorphic redundancy can be easily designed by a simple permutation of the states in the state table of a sequential circuit. It will be functionally identical to that of the original register but structurally different [4].

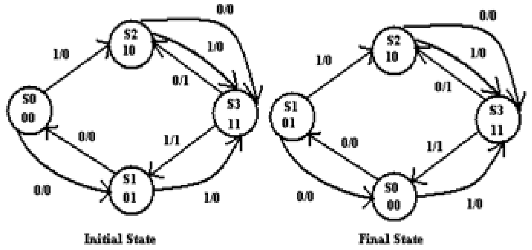


Fig.4 Isomorphic Redundancy

As in Fig.4 state S$_1$ is just swapped by the S$_0$ state but input and output assignments remains as it is same so this is an example of isomorphic redundancy. So an isomorphic redundant circuit is functionally equivalent also.

IV. PROPOSED WORK

We proposed a new type of redundancy in the shift register. Here not only swapping of sates is achieved but also all the original sequences are negated keeping all the input & output assignments same. That is we will get same output as original scan registers providing the same corresponding Input. Later one much more randomized redundancy is introduced, where the swapping of all the states is randomized to some extent & similarly all the input output assignments remains as it is same as original scan register. The scan registers where these type redundancies are implemented are called as *redundant shift registers (RSR)* that are functionally equivalent but not structurally equivalent to original scan registers. Using the *redundant scan registers (RScR)*, we present a new secure and testable scan design approach which satisfies both testability and security of digital circuits. The approach is only to replace the original scan registers to modified scan registers called *redundant scan registers (RScR)*.It also have two modes in which the circuitry is operated. One is *test mode* and another one is *system mode*, by adding an extra input called *control input* which switches the circuit between *test mode* and *system mode* .When set 0 to *control input* the circuitry switches to *test mode* and a tester can check the original sequences of the scan register and when set 1 to *control input* circuitry switches to *system mode* and the circuitry transferred to be redundant, states are swapped and the original sequences of the scan registers are negated.

A.Redundancy & RScR (Redundant Scan register)

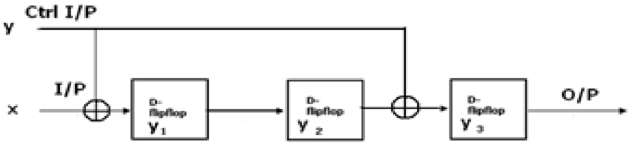


Fig5. abc$_2$ Scan register

Fig.5 shows the Redundant Scan register (*RScR*) which is functionally equivalent to the Scan register shown in Fig.1. As a result states will be swapped & sequences of original

DOI: 01.IJSIP.03.01.81

scan registers are negated which we have implemented in *system mode* and in *test mode* sequence remains as it is same as original scan register of Fig. 1 is represented by the de Bruijn graph. Where the state in *test mode* and *system mode* are shown in Fig. 6 as state in *test mode* /state in *system mode* fashion.

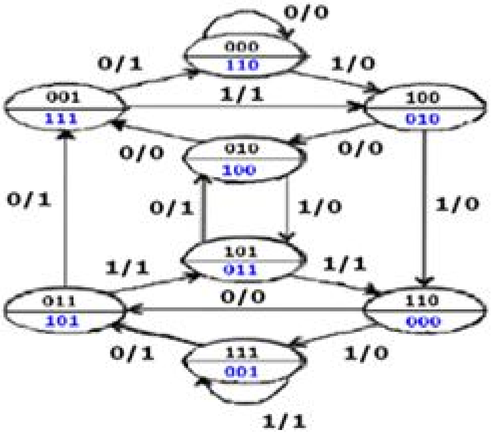


Fig.6 de Bruijn graph of fig. 5 in test mode/system mode fashion

The corresponding state table in *test mode* and *system mode* are illustrated in Table 2 and Table 3.

TableII. State table in test mode

XY	00	10
$Y_1Y_2Y_3$		
S_0 (000)	S_0/0	S_4/0
S_1 (001)	S_0/1	S_4/1
S_2 (010)	S_1/0	S_5/0
S_3 (011)	S_1/1	S_5/1
S_4 (100)	S_2/0	S_6/0
S_5 (101)	S_2/1	S_6/1
S_6 (110)	S_3/0	S_7/0
S_7 (111)	S_3/1	S_7/1

TableIII. State table in system mode

XY	01	11
$Y_1Y_2Y_3$		
S_0 (000)	S_5/0	S_1/0
S_1 (001)	S_5/1	S_1/1
S_2 (010)	S_4/0	S_0/0
S_3 (011)	S_4/1	S_0/1
S_4 (100)	S_7/0	S_3/0
S_5 (101)	S_7/1	S_3/1
S_6 (110)	S_6/0	S_2/0
S_7 (111)	S_6/1	S_2/1

But from security point of view it seems to be not so secured as if an intelligent hacker goes through the statistics of the state table for large number of times then he can eventually find that states are changed as the first two bits are negated, so then we propose another type of improved redundant design which increases the randomness of the changing of the sequences of scan registers. Like previous design it also consist two types of inputs depending on the *control input*, it switches between *testing mode* and *system mode*, when *control input (Y)* is 0 this circuit moves to the *testing mode* and when *control input (Y)* is 1 it moves to *system mode* is shown in Fig. 7.

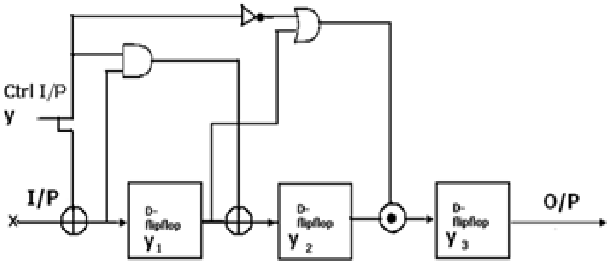


Fig7. abc$_3$ Scan register

The corresponding de Bruijn graph of this *RScR* is in Fig.8. The state in *test mode* and *system mode* are shown in Fig.8 State as in *test mode* /state in *system mode* fashion.

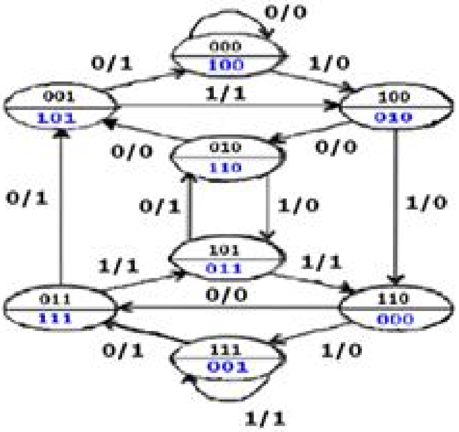


Fig8. de Bruijn graph of fig7. in test mode/system mode fashion

The state table in *test mode* and *system mode* illustrated in Table 4 and Table 5 respectively.

Table IV: State table in test mode

XY	00	10
$Y_1Y_2Y_3$		
S_0 (000)	S_0/0	S_4/0
S_1 (001)	S_0/1	S_4/1
S_2 (010)	S_1/0	S_5/0
S_3 (011)	S_1/1	S_5/1
S_4 (100)	S_2/0	S_6/0
S_5 (101)	S_2/1	S_6/1
S_6 (110)	S_3/0	S_7/0
S_7 (111)	S_3/1	S_7/1

DOI: 01.IJSIP.03.01.81

TABLE V: STATE TABLE IN SYSTEM MODE

XY	01	11
$Y_1Y_2Y_3$		
S_0 (000)	S_7/0	S_1/0
S_1 (001)	S_7/1	S_1/1
S_2 (010)	S_6/0	S_0/0
S_3 (011)	S_6/1	S_0/1
S_4 (100)	S_4/0	S_2/0
S_5 (101)	S_4/1	S_2/1
S_6 (110)	S_5/0	S_3/0
S_7 (111)	S_5/1	S_3/1

So in the *test mode* the circuit operates as the original normal shift register circuit in Fig. 1, so a tester can effectively check the circuit for testing. Now from Fig. 8 it is obseved that the sequences of the sequential circuit is one bit or in some cases two bit differnciating means often first one bit is negated or two bit is negated and from the state table we can find that swaping is also randomized , there is no certain rule for swaping the sequences of the shift register**,** so an intelligent hacker can never get any chance to hack in the scan chain.

B. RScR Added Scan Tree

Now as we know any scan chain can be represented by a tree shaped structure [5].

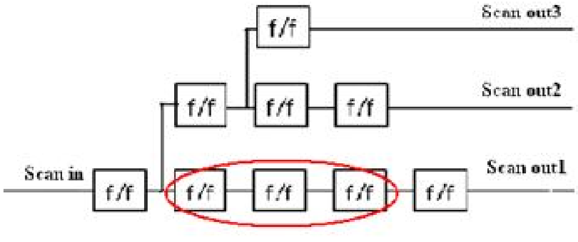


Fig9. Tree shaped scan chain

If we replace the circled 3 state scan register of fig. 9 by *RS_cR* (abc$_3$ scan register) as a result randomness and nonlinearity both will be introduced. The modified scan tree structure consists of both redundant and normal Scan D-flip-flops. The new scan tree continues to provide same amount of controllability and observability to the designer but not to the attacker. As the structure of the *RScR* and the structure of the scan tree are not known to the attacker. This makes it hard for the attacker to comprehend the structure of the tree. Further the new scan tree does not require an on-chip source or sink.

V. SECURITY & TESTABILITY

A circuit may consist of a single or multiple scan registers and the remaining combinational logic circuit (*kernel*) [9]. A scan register is nothing but a shift register with multiplexers that select the normal data from the combinational logic circuit and the shifting data from the preceding flip-flop. Here, we have replaced the shift register with a *redundant shift register (RSR)*.

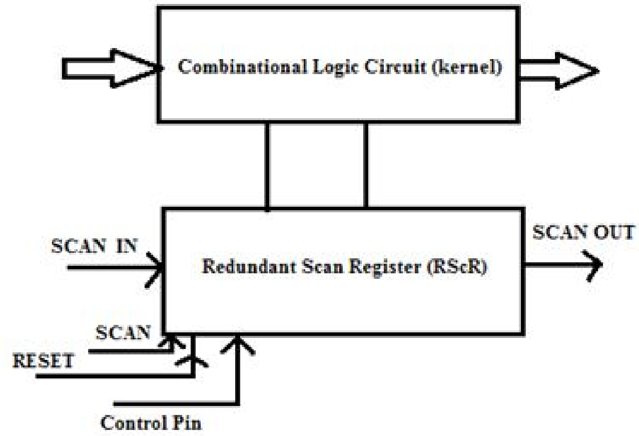

Combinational Logic Circuit (kernel)
SCAN IN
Redundant Scan Register (RScR)
SCAN OUT
SCAN
RESET
Control Pin

Fig10. Implementation of *RScR*

The scan register with the redundant shift register as shown in fig. 10 is called the redundant *scan register (RScR). S*can chains are proven to be effective in improvingthe testability of digital circuits. But as it possesses full controllability and observability on the circuit, which allow attackers to exploit this opportunity to extract key streams and even, manipulate the circuit. This makes it difficult for scan chains to be used especially in special cryptographic circuits where secret key streams are stored in internal registers, thus a problem in testing these types of circuits is imminent. However, quality of these circuits is highly in demand currently due to the increasing need of secure systems. Thus secure scan design through (*RScR)* provides both security and testability. With the same effectiveness and efficiency of conventional scan design and with very minimal overhead, any digital circuit can be both easily testable and secure against attackers.

When we consider a secure scan design, we need to assume what the attacker knows and how he can potentially make the attack. Here, we assume the following.

A. ATTACKER'S KNOWLEDGE

a) The attacker does not know the detailed information in the gate-level design.

b) The attacker knows the cryptographic algorithm implemented in the circuit. So he can make *bit-change insertion attack or differential values attack* [1].

c) The attacker knows the presence of test pins (scan-in/out, scan, and reset) and scan chains. However, he does not know the structure of *RScR* (the connection information, positions of XOR and NOT, and the size) and the presence of the control pin .Based on the above assumptions, we define the security to prevent scan-based side-channel attacks.

The structure of the *RScR* is important to the attacker in order to understand the scanned out values from the registers, which can reveal the key stream or the initial values of the internal registers, once computed. Thus, the level of security is dependent on the difficulty of determining the *RScR* structure. If the attacker cannot identify the structure of the *RScR*, the internal register values cannot be retrieved as output would remain the same as it would for conventional scan fig. 6 and fig. 8 shows the de Bruijn graph of two different types of *RScR* (abc2, abc3). that are all functionally

DOI: 01.IJSIP.03.01.81

equivalent to the 3-stage shift register but their state assignments are different and hence the content of each register cannot be observed from the input/output sequence in *system mode* while served to the customers.

B. Security Analysis of Stream Cipher with RSR added-Scan Tree :

Now in case of stream cipher the structure of scan chain can be determined only if the user feeds in values of his choice and analyze the scan out data. Now with *RSR added scan tree* structure the attacker is deprived of knowing the sequences of the scan chain.

C. Security Analysis of AES with RSR added-Scan Tree :

AES is an encryption standard used by the U.S. government since 2001. It is now one of the most popular block cipher techniques due to its simple implementation in hardware. Each AES [8] encryption includes several rounds, and each round consists of four basic operations:

a) The Byte Sub Transformation;

b) Shift Row Transformation;

c) Mix Column Transformation and

d) Add Round Key.

In the last operation, Add Round Key, data is exclusive- ORed with a predefined encryption key. The length of the encryption key can be chosen as 128, 196, or 256 bits. AES algorithm is a private key encryption, which means the encryption key (same as the decryption key) is between the transmitter and the receiver only. Any leakage of the encryption key results in a serious security problem. Conventional block ciphers like AES are insecure under scan chain based attacks [1]. In order to prevent scan based attacks on AES, we have inserted the *RScR added scan tree* for registers that need to be secured in AES hardware. In the following we show that the *RScR added scan tree* architecture provides high security with very low overhead.

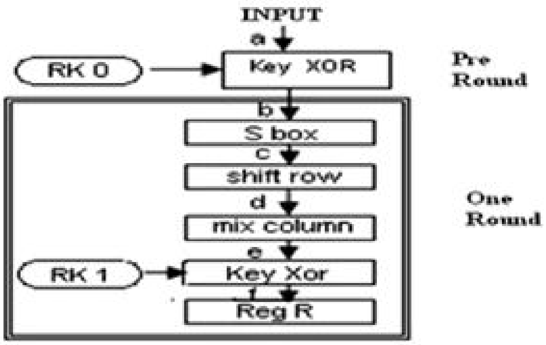


Fig.11 Round Operation of AES encryption

Now the attack on AES by [6] only can crack if it gets the following information: The first step is to guess the position of the registers to obtain intermediate values of each step. The main motive is to find the position of the register R in the above figure by exploiting the property of Avalanche effect in good ciphers. Once, the position of register R was ascertained the second step comes to play. In this step, two values of input plaintext were chosen which differs in one byte. From the number of 1's in the XOR of the scanned out values of the register R and differential property of the AES algorithm, the values of register b was computed. Finally, using value of **a** and the register b the key value was calculated using: RK0=B Å A. In our *RScR* added scan chain architecture such an attack is not viable because of the presence of the *RScR* and the nonlinear scan tree. The security of the structure is due to the following reasons: Attacker cannot ascertain the position of register R due to the unknown linear structure of the scan tree. The presence of RSR in the scan path does not allow ascertaining the structure of the tree. This is because the attacker has no control over the input to the internal structures of the design until he knows the full structure of the RSR added scan tree. Since step 1 fails, step 2 cannot be performed. Also, it may be noted that step 2 is also not possible. This is because the attacker requires computing differences in the scanned out values of register R, which is now obscured by the non-linear property of the RSR added-scan tree. Hence the system is secure against the known scan chain based attacks.

VI. THE ADVANTAGES OF RScR ADDED SCAN TREE

Apart from providing high securities to the designs, following are enlisted the other advantages of the *RScR added scan tree*.

Fast Testing: Due to the tree structure the testing is fast.

High Fault coverage: The *RScR added* scan chain has the same amount of controllability and observability as conventional scan chain for the designer. Since the designer don't have to aware of the positions of the *RScR* in the *RScR added scan tree* structure as in test mode he will get the original sequences as an original shift register, he can easily feed in patterns and observe the intermediate values of the system and thereby test the system accurately.

On-line testing is possible: There is no need of turning off the system before testing the circuit unlike in the case of secure scan architecture

Testing of additional circuits or inverters is easy: Since the additional circuitry involves combinational units, testing can be easily performed.

VII. The Probability Of Determining The Structure Of The RSR Added Scan Tree

The probability of guessing the correct structure of the scan tree is [5]

$$1 \ / \sum_{L}^{NL} ({}^{NL}C_r * r^{r-2} * 2^r) \qquad (1)$$

The probability of guessing the correct structure of the *RScR* is

$$1 / \sum_{i=1}^{K} 2^K \qquad (2)$$

as the hacker knows nothing about length of our *RScR* or about the degree of *RScR* , then he has to try exhaustively all bit sequences of lengths 1 to K .

DOI: 01.IJSIP.03.01.81

Hence the total probability of guessing the correct structure of the *RScR added scan tree* is

$$1 \ / \{ \sum_{L}^{NL} ({}^{NL}C_{r} * r^{r-2} * 2^{r}) * \sum^{K} 2^{K} \}_{i=1} \tag{3}$$

Where

N: Is the number of scan output pins

L: Is the depth of the scan tree

r: Is the number of nodes

K: Is the K stage shift register

VIII. AREA COST & TEST POWER

To reduce the overhead due to many feed-forwards and feedbacks in a long scan chain, we can use a shift register (standard scan register) for the non-secure part that is not required to be scan-secure. As for the influence on test power due to shift register modification, the insertion of inverters AND/OR/ XOR gates can reduce test power even more than standard scan design if they are inserted appropriately as mentioned.

CONCLUSION

A new secure scan design has been introduced. It involves modification of original scan registers of scan design to redundant scan registers *(RScR)*. One type has been analyzed for scan-testability and scan-security.*RScR added scan tree* of a shift register can be both scan-testable and –secure by adding one extra *control line input*. A long secure scan chain can be easily constructed by cascading short scan-testable and scan-secure *redundant shift registers*. It also does not involve the use of additional key streams. Therefore, it provides an efficient solution to satisfy both testability and security with lesser cost.

REFERENCES

[1] Bo Yang, Kaijie Wu, and Ramesh Karri “Secure Scan: A Design-for-Test Architecture for Crypto Chips” Publication Year: 2006, Page(s): 2287 - 2293.

[2] David Hély1&2, Frédéric Bancel1, Marie-Lise Flottes2, Bruno Rouzeyre 2 “Test Control for Secure Scan Designs” Publication Year: 2005, Page(s): 190 – 195.

[3] *David Hély1, Marie-Lise Flottes2, Frédéric Bancel1, Bruno Rouzeyre2, Nicolas Bérard1, and MichelRenovell2.*”Scan Design and Secure Chip” Publication Year: 2004, Page(s): 219 – 224.

[4] Debesh K. Das, Uttam K. Bhattacharya, andBhargab B. Bhattacharya,”Isomorph-Redundancy in Sequential Circuits” Publication Year: 2000 , Page(s): 992 - 997.

[5] Gaurav Sengar, Debdeep Mukhopadhayay, D Roy Chowdhury “An Efficient Approach to Develop Secure Scan Tree for Crypto-Hardware” Publication Year: 2007, Page(s): 21 – 26.

[6] Hideo Fujiwara and Marie Engelene J. Obien “Secure and Testable Scan Design Using Extended de Bruijn Graphs” Publication Year: 2010, Page(s): 413 – 418.

[7] Jeremy Lee, Mohammed Tehranipoor, Chintan Patel, and Jim Plusquellic “Securing Scan Design Using Lock & Key Technique” Publication Year: 2005, Page(s): 51 – 62.

[8] J. Daemen and R. Rijmen, “*The Design of Rijndael: AES—The Advance Encryption Standard*.” Berlin, Germany: Springer-Verlag, 2002, pp. 31–62.

[9] Michiko Inoue Tomokazu Yoneda Muneo Hasegawa Hideo Fujiwara “Partial Scan Approach for Secret Information Protection “ Publication Year: 2009, Page(s): 143 – 148.

[10] Somnath Paul, Rajat Subhra Chakraborty and Swarup Bhunia “VIm-Scan: A Low Overhead Scan Design Approach for Protection of Secret Key in Scan-Based Secure Chips” Publication Year: 2007, Page(s): 455 – 460.

DOI: 01.IJSIP.03.01.81